Romain Jacquet **BTS SIO 1**
27/11/2025

Compte rendu TP TH2 : CH3 TD2

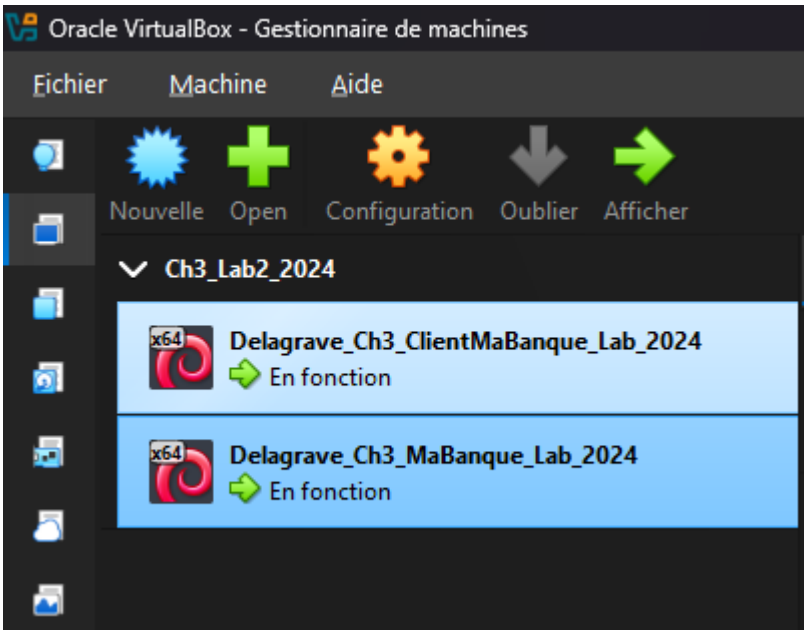
Sommaire

Introduction

Dans ce TP, j'ai mis en place un petit environnement de messagerie entre deux machines virtuelles afin de comprendre comment sécuriser des échanges par email. Après avoir configuré VirtualBox, Thunderbird et les adresses mail, l'objectif était d'apprendre à utiliser le chiffrement PGP pour protéger les messages et vérifier leur authenticité.

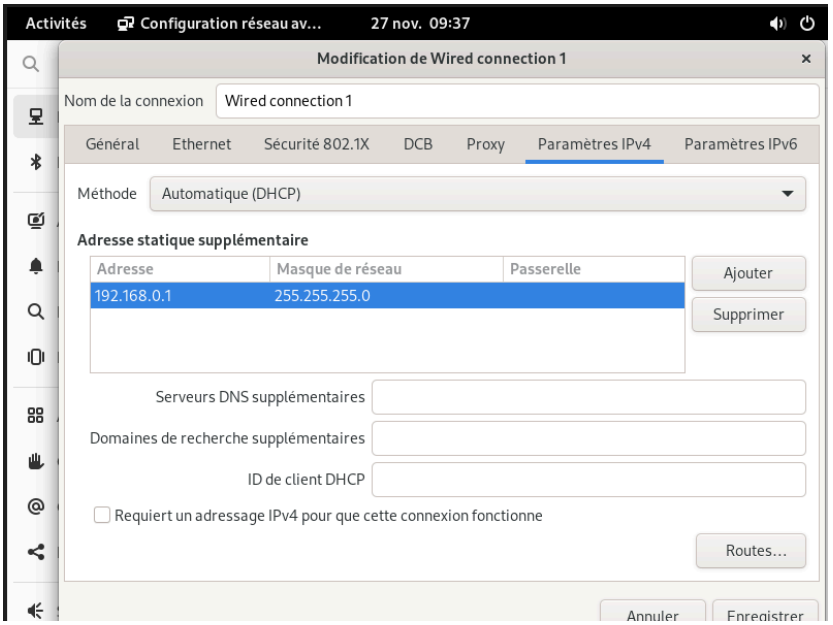
1.

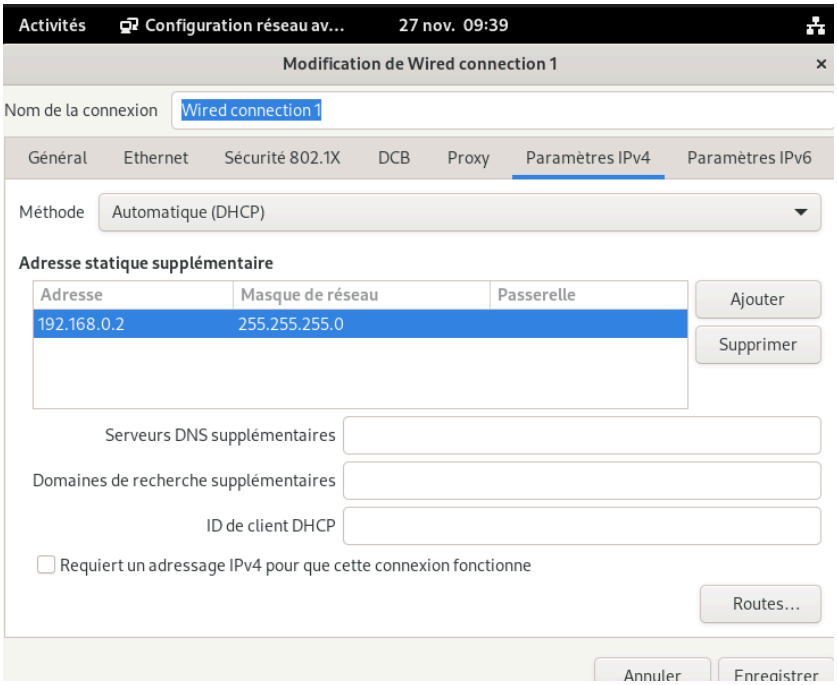
J’ai importé les 2 machines virtuelles dans le logiciel VirtualBox



2.

J’ai commencé par paramétrer le réseau des 2 VM avec les adresses IP fournies.





Ensuite j'ai créé les adresse mail de messagerie Thunderbird
J'ai lancé l'application Thunderbird sur chaque machine et j'ai procédé aux trois ajustements demandés :

- Créer les deux adresses de messagerie : J'ai suivi l'assistant de configuration de compte de Thunderbird. J'ai créé les adresses virtuelles : `mabanque@gmail.com` et `clientmabanque@gmail.com`.
- Créer un compte de messagerie pour chaque utilisateur : Lors de la création, j'ai fait attention à donner le nom de compte approprié pour la gestion interne de Thunderbird : `MaBanque` et `Client-MaBanque`.
- J'ai modifier les paramètres pour choisir la langue de l'interface :

    Je suis allé dans le menu « Paramètres » (ou `Préférences`).

    Dans les paramètres généraux, j'ai recherché l'option de « Langue » ou « Apparence ».

    J'ai sélectionné le Français (France) pour m'assurer que les options de chiffrement qui arriveront plus tard soient clairement affichées dans la bonne langue.

3.

J’ai testé l'envoi de courriels entre les deux acteurs et vérifier si le contenu du message est crypté.

J'ai juste envoyé un email classique pour voir si tout fonctionnait et surtout, pour confirmer qu'on n'avait aucune sécurité pour l'instant.

- J'ai pris la machine M@Banque, j'ai tapé un message test à l'adresse du client (`clientmabanque@gmail.com`), et j'ai cliqué sur "Envoyer".
- Je suis allé sur la machine ClientM@Banque, et j'ai immédiatement reçu le message.La communication passe bien !

J'ai ouvert l'email reçu, et sans surprise, j'ai lu le contenu clairement.

Donc le message n'était PAS crypté (ou chiffré).

4.

Pour paramétrer le chiffrement de bout en bout pour les deux utilisateurs.

J'ai donné à chaque utilisateur sa propre clé secrète et j'ai organisé un échange de clés publiques. C'est l'étape la plus importante pour la sécurité !

- J’ai fabriqué des Clés : Sur chaque machine (M@Banque et le Client), en utilisant le menu « Paramètres » pour générer une paire de clés OpenPGP (une clé secrète, qui reste cachée, et une clé publique).
- L'Échange : J'ai ensuite envoyé la clé publique de M@Banque au Client (par email, via le Gestionnaire de clés OpenPGP) et j'ai fait l'inverse.
- L'Installation : Dès réception, j'ai importé la clé de l'autre dans le gestionnaire de clés de chaque machine.

Maintenant, les deux ordinateurs ont la "clé de boîte aux lettres" de l'autre. Ils peuvent désormais crypter un message que seul le destinataire pourra ouvrir. La sécurité est prête !

5.

Pour tester l'envoi de courriels cryptés et vérifier la sécurité.

J'ai envoyé un email important depuis M@Banque, mais cette fois-ci, j'ai activé le chiffrement PGP.

- L'Envoi : J'ai composé le message et je me suis assuré que le bouton "Crypter" était bien enclenché avant de l'envoyer au Client.

- La Réception : Sur la machine du Client, le message est arrivé.

Ca marche car :

- Le Client lit le message : Il a pu le déchiffrer sans problème grâce à sa clé secrète.
- Le Cadenas est là : Thunderbird montre une icône de cadenas fermé (ou un bandeau clair) confirmant que le message a été protégé par PGP.

Donc la confidentialité est assurée. Le contenu est illisible par toute personne autre que le destinataire.

6.

Le chiffrement (Étape 4) rend le message confidentiel (personne ne peut le lire). Mais la signature, c'est différent.

- À quoi ça sert ? La signature prouve qui on est vraiment (l'authenticité) et garantit que le message n'a pas été modifié pendant le transfert (l'intégrité).
- Pourquoi l'utilisateur doit le faire ? Il utilise sa clé secrète pour signer, ce qui est un acte d'engagement. S'il signe, il ne peut plus nier plus tard avoir envoyé ce message. C'est essentiel pour en faire un moyen de preuve sécurisé.

7.

Mission pleinement réussie : après avoir installé notre labo virtuel dans VirtualBox et configuré un réseau IP statique ainsi que les comptes Thunderbird, nous avons vérifié que les messages circulaient bien en clair avant de passer à l’étape cruciale de la génération et de l’échange des clés PGP ; une fois ce prérequis rempli, le test a confirmé que les emails étaient correctement chiffrés, garantissant leur confidentialité, et la signature PGP est venue compléter le dispositif en assurant l’authenticité et la non-répudiation des messages grâce à la clé secrète ; enfin, le rapport final atteste que cette procédure constitue une solution fiable et parfaitement adaptée pour des communications sécurisées à haute valeur probatoire.

Conclusion

Au final, tout fonctionne comme prévu : les deux machines peuvent s’envoyer des messages chiffrés et signés, ce qui garantit que seuls les destinataires peuvent les lire et que l’expéditeur est bien celui qu’il prétend être. Ce TP m’a permis de mieux comprendre comment fonctionne la sécurité dans les échanges mails et pourquoi ces mécanismes sont importants au quotidien.